CHAPTER 11

Physical Security of Personnel and Equipment

11-100 Physical Security Policy

1. It is recognized that AFRTS outlets are located in many geographical areas of the world that, at some time, could become subject to hostile actions between opposing forces and/or subject to terrorist threats or actions. AFRTS policy is to protect at all times, to the maximum extent possible, all assigned personnel, equipment, and facilities from hostile and/or terrorist threats or actions. While 100 percent protection against terrorist activities can never be guaranteed, several things can and should be done to lessen the degree of exposure to hostile force and/or terrorist threats.

11-101 Security Responsibilities

1. Network Commanders and/or Station Managers shall, in full coordination with their host-command and respective Broadcasting Service, ensure that plans and/or procedures for protecting against hostile threats and/or actions are addressed in Host-Tenant Support Agreements, Memorandums of Understanding and/or Inter-Service Support Agreements. This is a mandatory requirement. These protective plans and/or procedures must be based on various factors, which include mission requirements, available personnel resources, fiscal resources, host-command support, Unified/Specified Command and theatre commander requirements, and the severity of either imminent or long-term threats. Each Broadcasting Service shall have on file a copy of the physical security plans and/or procedures for each outlet under its control.

11-102 Minimum Physical Security Requirements

1. Each overseas AFRTS outlet (no matter where located and including remote transmitter facilities) shall be provided, by the agency responsible for the site's operation and maintenance, the following minimum protection:

a. A simple duress alarm system at studio and manned transmitter locations. An intrusion alarm system at all remote unmanned transmitter facilities.

b. Outdoor security lighting.

c. Security bars on all windows (or 'equivalent).

d. A cypher lock on primary access door and adequate locking devices on all interior doors.

2. All AFRTS Station Managers shall:

a. Have a valid physical security plan that' realistically reflects local conditions and possible local threat environment.

b. Ensure that the station security plan is incorporated into the host-command security plans and/or procedures.

c. Review the station physical security plan annually and have it evaluated by a disinterested party.

d. Make certain that the host-command security police adequately check station security during their routine patrols and provide them with any special instructions.

e. Provide a copy of any security plan changes to their appropriate Broadcasting Service headquarters.

3. Physical Security plans and/or procedures must address at least the following areas:

a. Station access procedures. Access to AFRTS outlets must be tightly controlled at all times, even when there is no threat. In times. of threat, use of access lists, 100 percent ID card checks, and increased use of security personnel may be appropriate. Measures that would deny unauthorized persons access to the station after an evacuation are also required.

b. Protection of assigned personnel. Personnel should be evacuated before the station is under a direct threat. In the early stages of a threat condition, station operations should be reduced to allow for the early evacuation of as many personnel as possible. Actions that involve unnecessary risk to station personnel shall be avoided. Each station must have a pre-designated safe-haven where evacuated personnel can gather and an established procedure of accounting for assigned personnel. ‘

c. Station disablement. Station disablement procedures must reflect safety considerations, require only minimum technical knowledge, and avoid irreparable damage. Station disablement should be undertaken only when competent senior military authority in the operational chain-of-command has determined that enemy and/or terrorist takeover of the station is imminent.

d. Protection, removal and/or destruction of AFRTS program materials. The security plan must provide for the safeguarding, removal, or destruction of AFRTS program materials. There should be no hesitation about destroying the program materials if the situation so warrants.

e. Protection, removal, and/or destruction of all broadcast equipment. The security plan must address proper procedures for removing the broadcast equipment to a safe location before the takeover of a station becomes imminent, or the equipment must be destroyed if there is not enough time to remove it to a safe location.

f. Protection, removal, and/or destruction of key documents. Operational Plans (OPLANS), Standard Operating Procedures (SOP’s), transmitter schematics, technical manuals, wiring diagrams, facility records, or other. key documents that could possibly be used by hostile enemy and/or terrorist personnel to conduct broadcast operations must be removed or destroyed.

g. Chain-of-command notification procedures. The security plan must contain procedures for notifying the operational chain-of-command when the enemy and/or antiterrorism plan is activated. Network Commanders must assume that they may not be able to alert their affiliate stations through normal communication channels.

4. The AFRTS outlet (Station) Security Plan must acknowledge that the outlet may be required to continue operations (perhaps in a non-standard operating manner, i.e., automation system with recorded advisories, cable operation only, etc.) for as long as possible during a threat situation. Host-command base security plans should delineate the support required of the AFRTS outlet in abnormal situations. The base hostage negotiation team should be familiar with the outlet's capabilities and be allowed access to the outlet to support its activities. In any abnormal situation, every effort shall be made to support the host-command base actions, consistent with DoD Directive 5120.20 (reference (a)).